Checkliste: Wie gehe ich mit IT-Risiken um?

Der richtige Umgang mit IT-Risiken ist für Unternehmen eine Überlebensfrage. Um so wichtiger ist eine Risikoanalyse, mit Sie die Risiken erkennen, den Schutzbedarf ermitteln und so möglichen Schäden vorbeugen können. Auch rechtliche Auflagen gilt es zu erfüllen und Haftungsfragen zu klären. Die Checkliste hilft Ihnen dabei.

Risiken erkennen

- ○ Kennen Sie die rechtlichen Anforderungen im Zusammenhang mit Ihrer IT? Z.B.
  - □ Anforderungen des Datenschutzes (z.B. auch Bestellung eines Datenschutzbeauftragten)
  - □ Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)
  - □ Branchenspezifische Regelungen (z.B. im sozialen Bereich)
  - □ Vertragliche Regelungen (z.B. Vertraulichkeitsvereinbarungen, IT-Outsourcing)
- ○ Haben Sie Rat von Dritten eingeholt (Expertise, Sicht eines Betriebsfremden)?
- ○ Haben Sie für Ihre wichtigen IT-Anwendungen identifiziert,
  - □ welche IT-Systeme dafür notwendig sind?
  - □ welche Daten in diesen Anwendungen verarbeitet werden?
  - □ wo und wie die Hardware für diese Systeme aufgestellt ist?

Risiken bewerten

- ○ Haben Sie überprüft, was für Schäden eintreten können?
  - □ Schäden, die durch Nichtverfügbarkeit von Daten und Systemen entstehen (z.B. wenn Daten „verschwunden“ sind, die Kommunikation wie z.B. E-Mail nicht funktioniert)
  - □ Schäden, die durch fehlerhafte (manipulierte) Daten entstehen können (z.B. durch frustrierte Mitarbeiter oder durch Schadsoftware)
  - □ Schäden, die durch Verletzung von Betriebsgeheimnissen entstehen können (z.B. Entwürfe, Angebote oder Prozessbeschreibungen)

- Haben Sie sich einen Überblick über mögliche Schadenshöhen verschafft?
  - Schadenshöhen bei Ausfall der Hardware oder Software
  - Schadenshöhen bei Datenverlust
  - Schadenshöhen durch „Datendiebstahl“ (z.B. unbefugte Einsichtnahme, Kopieren)
- Haben Sie Schadenskategorien festgelegt, wie etwa „Schaden darf nicht eintreten“, „hoher Schaden“, „niedriger Schaden“ oder auch nach „Schulnoten“?
- Haben Sie eine Liste der potenziellen Schäden erstellt und diese den Kategorien zugeordnet?
- Haben Sie für jeden dieser möglichen Schäden eine Eintrittswahrscheinlichkeit festgelegt?
- Haben Sie die Schwachstellen Ihrer IT identifiziert?
- Haben Sie geprüft, ob Ihre vorhandenen Schutzmaßnahmen ausreichen?

Sicherheitsmaßnahmen

- Haben Sie sich über notwendige Sicherheitsmaßnahmen informiert und auch z.B. „best practices“ berücksichtigt?
- Haben Sie geprüft, ob eine Änderung der Arbeitsabläufe das Risiko minimieren kann?
- Haben Sie geprüft, ob Sie Versicherungen gegen etwaige Risiken abschließen können?
- Haben Sie geprüft, ob Sie risikobehaftete Prozesse an externe Dienstleister auslagern können?

Weitere Informationen zum Thema IT-Risikoanalyse finden Sie in unserem Flyer:

„IT-Risiken erkennen und vermeiden – 10 Praxistipps für kleine und mittlere Unternehmen und das Handwerk”

Das Netzwerk Elektronischer Geschäftsverkehr

Seit 1998 berät und begleitet das Netzwerk Elektronischer Geschäftsverkehr, in 27 über das Bundesgebiet verteilten regionalen Kompetenzzentren und einem Branchenkompetenzzentrum für den Handel, Mittelstand und Handwerk bei der Einführung von E-Business Lösungen. In dieser Zeit hat sich das Netzwerk mit über 30.000 Veranstaltungen und Einzelberatungen mit über 300.000 Teilnehmern als unabhängiger und unparteilicher Lotse für das Themengebiet „E-Business in Mittelstand und Handwerk“ etabliert. Das Netzwerk stellt auch Informationen in Form von Handlungsanleitungen, Studien und Leitfäden zur Verfügung, die auf dem zentralen Auftritt www.ec-net.de heruntergeladen werden können. Die Arbeit des Netzwerks wird durch das Bundesministerium für Wirtschaft und Technologie gefördert.

Sichere E-Geschäftsprozesse in KMU und Handwerk

Die Checkliste IT-Sicherheit wurde im Rahmen des Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk“ des Netzwerks Elektronischer Geschäftsverkehr (NEG) erstellt. Das Verbundprojekt wird vom Bundesministerium für Wirtschaft und Technologie (BMWi) unterstützt und soll helfen, in kleinen und mittleren Unternehmen mit verträglichem Aufwand die Sicherheitskultur zu verbessern. Hier werden insbesondere kleine und mittelständische Unternehmen sowie das Handwerk zu wichtigen Aspekten der Informationssicherheit sensibilisiert und praxisnah informiert. Alle Details finden Sie unter: www.kmu-sicherheit.de

TeleTrusT – Bundesverband IT-Sicherheit e.V.

TeleTrusT wurde 1989 gegründet, um verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik zu schaffen. TeleTrusT entwickelte sich zu einem bekannten Kompetenznetzwerk und trägt seit 2011 die Bezeichnung „TeleTrusT – Bundesverband IT-Sicherheit e.V.“. Heute umfasst TeleTrusT mehr als 130 institutionelle Mitglieder. Die Mitgliederschaft setzt sich aus Industrie, insbesondere mittelständischen Unternehmen, Bundesbehörden, Forschungseinrichtungen und thematisch verwandten Organisationen aus Deutschland, Österreich, der Schweiz, Belgien, Frankreich und Großbritannien zusammen, was die allgemeine Bedeutung des Themengebietes IT-Sicherheit unterstreicht. TeleTrusT hat Gemeinnützigkeitsstatus. In Arbeitsgruppen zu aktuellen Themen der IT-Sicherheit und des Sicherheitsmanagements findet interdisziplinärer Erfahrungsaustausch statt. TeleTrusT äußert sich zu technischen, politischen und rechtlichen Fragen, organisiert Veranstaltungen und Veranstaltungsbeteiligungen und ist Trägerorganisation der „European Bridge CA“ (Bereitstellung von Public-Key-Zertifikaten für sichere E-Mailkommunikation) sowie des Zertifikates „TeleTrusT Information Security Professional“ (T.I.S.P.). Hauptsitz des Verbandes ist Berlin. TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Weitere Informationen finden Sie unter: www.teletrust.de